EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Pehr Jansson on November 4, 2008.

The application has been amended as follows:

Claims 1, 2, 4, 6, 7, 9 – 16, 61, 62, 64, 66 - 69, and 71 - 76 are amended. Claims 18 - 60, 78 and 79 have been cancelled. Claims 80 - 113 are new.

Claims:

1. (CURRENTLY AMENDED) A method of secure communication between a ~~resource-constrained device~~ smart card and remote network nodes over a network wherein the ~~resource-constrained device~~ smart card acts as a standalone network node and the remote network nodes communicate with the ~~resource-constrained device~~ smart card using un-modified network clients and servers and wherein the ~~resource-constrained device~~ smart card has a central processing unit, a random access memory, a non-volatile memory, a read-only memory, and an input and output component, comprising:

using a physical link selected from one of several physical link methods;

assigning a unique network address to the ~~resource-constrained device~~ smart card thereby enabling the ~~resource-constrained device~~ smart card to act as a standalone network node;

executing on the ~~resource-constrained device~~ smart card a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with a host computer, operable to communicate with remote network nodes using the networking protocols and operable to implement network security protocols thereby setting a security boundary inside the ~~resource-constrained device~~ smart card;

implementing an execution model, wherein the communication module is driven by input events and by the applications and wherein the ~~resource-constrained device~~ smart card optimized memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers;

executing on the host computer one or more communication and networking protocols operable to communicate with the ~~resource-constrained device~~ smart card and operable to communicate with the remote network nodes; and

executing one or more secure network applications on the ~~resource-constrained device~~ smart card wherein the network applications call upon the communication module of the ~~resource-constrained device~~ smart card to communicate with the host computer or the remote network node using the networking protocols and network security protocols and wherein the secure network applications are securely accessible by the remote network nodes using un-modified network clients and servers.

2. (CURRENTLY AMENDED) The method of Claim 1 wherein the physical link is selected from the set including full-duplex serial connection~~,~~ and half-duplex serial connection~~, USB connection, contactless radio connection~~.

3. (ORIGINAL) The method of Claim 2 wherein the physical link is a full-duplex serial connection using the serial peripheral interface protocol.

4. (CURRENTLY AMENDED)The method of Claim 1 further comprising connecting an interface device between the ~~resource constrained device~~ smart card and the host computer using a physical link that is a serial connection having half-duplex between the ~~resource constrained device~~ smart card and the interface device and full-duplex between the interface device and the host computer.

5. (ORIGINAL) The method of Claim 4 further comprising operating the interface device to perform a bridging function between the half-duplex connection and the full-duplex connection.

6. (CURRENTLY AMENDED) The method of Claim 5 wherein the step of performing a bridging function further comprises providing at least one of function selected from:

   enabling a ~~resource constrained device~~ smart card operating in a command/response mode to communicate with network nodes as a peer;

   enabling a ~~resource constrained device~~ smart card operating in half-duplex communication mode to handle full-duplex communication traffic;

   encapsulating upper layer protocol frames;

   enabling transportation of upper layer protocol frames exceeding a frame size limit of the lower link layer; and

supporting multiple logical connections of upper layer protocols.

7. (CURRENTLY AMENDED) The method of Claim 4 of operating a software module on the interface device according to a finite state machine permitting the interface device to forward messages between the ~~resource constrained device~~ smart card and the network wherein the interface device is in one of the at least one states permitting the ~~resource constrained device~~ smart card to initiate and send messages.

8. (ORIGINAL) The method of Claim 7 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

9. (CURRENTLY AMENDED) The method of Claim 4 of operating a software module on the host computer according to a finite state machine having at least one state permitting the ~~resource constrained device~~ smart card to transmit messages to the network wherein the software module is in one of the at least one states permitting the ~~resource constrained device~~ smart card to initiate and send messages.

10. (CURRENTLY AMENDED) The method of Claim 9 wherein the at least one state permitting the ~~resource constrained device~~ smart card to transmit messages to the network is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

11. (CURRENTLY AMENDED) The method of Claim 9 comprising the step of operating the ~~resource constrained device~~ smart card according to a finite

state machine having at least one state in which the ~~resource constrained device~~ smart card waits for a message from the host computer indicating that the ~~resource constrained device~~ smart card may transmit a message.

12. (CURRENTLY AMENDED) The method of Claim 4 further comprising:

operating the ~~resource constrained device~~ smart card according to a finite state machine whereby the ~~resource constrained device~~ smart card uses the response status at the end of the response to the command sent by the host computer or an intermediate device to indicate that the ~~resource constrained device~~ smart card wants to transmit information to the host computer or to the network.

13. (CURRENTLY AMENDED) The method of Claim 12 where in the step of operating the ~~resource constrained device~~ smart card comprises operating the ~~resource constrained device~~ smart card according to a finite state machine having at least one state in which the ~~resource constrained device~~ smart card waits for a message indicating to the ~~resource constrained device~~ smart card that the ~~resource constrained device~~ smart card may transmit information to the host.

14. (CURRENTLY AMENDED) The method of Claim 13 further comprising operating the ~~resource constrained device~~ smart card to transition among the states of the finite state machine.

15. (CURRENTLY AMENDED) The method of Claim 12 further comprising:

operating the host computer or an intermediate device connected between the host computer and the ~~resource constrained device~~ smart card according to a finite state machine to transmit a

polling message to the ~~resource constrained device~~ smart card checking if the ~~resource constrained device~~ smart card may want to transmit information to the host computer.

16. (CURRENTLY AMENDED) The method of Claim 15 wherein the host computer or intermediate device includes a Remote Access Server (RAS) and wherein the step of operating the host computer or intermediate device comprises operating the host computer or intermediate device according to a finite state machine having a Polling state in which the host computer or intermediate device polls the ~~resource limited device~~ smart card, a Get-from-card state in which the host computer or intermediate device obtains packets of data from the ~~resource constrained device~~ smart card, a Putting-to-card state in which the host computer or intermediate device transmits data to the ~~resource constrained device~~ smart card, and a Checking Remote Access Server(RAS) state in which the host computer or intermediate device checks whether Remote Access Server (RAS) has any data to transmit to the ~~resource constrained device~~ smart card.

17. (ORIGINAL) The method of Claim 16 further comprising operating the host computer or the intermediate device to transition among the states of the finite state machine.

18. – 60 (CANCELLED)

61. (CURRENTLY AMENDED) A system providing secure communication between a ~~resource constrained device~~ smart card and remote network nodes over a network wherein the remote network nodes communicate with the ~~resource constrained device~~ smart card using un-modified network clients and servers and wherein the ~~resource constrained device~~ smart card has a central processing unit, a random access memory, a

non-volatile memory, a read-only memory, and an input and output component, the system comprising:

a physical link connecting the ~~resource-constrained device~~ smart card and a host computer, the physical link selected from one of several physical link methods;

logic to assign a unique network address to the ~~resource-constrained device~~ smart card thereby enabling the ~~resource-constrained device~~ smart card to act as a standalone network node;

the ~~resource-constrained device~~ smart card comprising a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with the host computer, operable to communicate with remote network nodes using the networking protocols and operable to implement network security protocols thereby setting a security boundary inside the ~~resource-constrained device~~ smart card, wherein the communication module is driven by input events and by the applications and wherein the ~~resource-constrained device~~ smart card optimizes memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers;

the host computer comprising logic implementing one or more communication networking protocols operable to communicate with the ~~resource-constrained device~~ smart card and operable to communicate with the remote network nodes; and

the ~~resource-constrained device~~ smart card further comprising one or more secure network applications wherein the network applications call upon the communication module of the

~~resource constrained device~~ smart card to communicate with the host computer or the remote network node using the networking protocols and network security protocols and wherein the secure network applications are securely accessible by the host computer or the remote network nodes using un-modified network clients or servers.

62. (CURRENTLY AMENDED) The system of Claim 61 wherein the physical link is selected from the set including full-duplex serial connection~~,~~ and half-duplex serial connection, ~~USB connection, contactless radio connection~~.

63. (PREVIOUSLY PRESENTED) The system of Claim 62 wherein the physical link is a full-duplex serial connection using the serial peripheral interface protocol.

64. (CURRENTLY AMENDED)The system of Claim 61 further comprising an interface device between the ~~resource constrained device~~ smart card and the host computer, the interface device using a physical link that is a serial connection having half-duplex between the ~~resource constrained device~~ smart card and the interface device and full-duplex between the interface device and the host computer.

65. (PREVIOUSLY PRESENTED) The system of Claim 64 further wherein the interface device comprises logic to perform a bridging function between the half-duplex connection and the full-duplex connection.

66. (CURRENTLY AMENDED) The system of Claim 65 wherein the logic to perform a bridging function further comprises logic to provide at least one of function selected from:

enabling a ~~resource constrained device~~ smart card operating in a command/response mode to communicate with network nodes as a peer;

enabling a ~~resource constrained device~~ smart card operating in half-duplex communication mode to handle full-duplex communication traffic;

encapsulating upper layer protocol frames;

enabling transportation of upper layer protocol frames exceeding a frame size limit of the lower link layer; and

supporting multiple logical connections of upper layer protocols.

67. (CURRENTLY AMENDED) The system of Claim 64 wherein the interface device further comprises logic to operate the interface device according to a finite state machine permitting the interface device to forward messages between the ~~resource constrained device~~ smart card and the network wherein the interface device is in one of the at least one states permitting the ~~resource constrained device~~ smart card to initiate and send messages.

68. (CURRENTLY AMENDED) The system of Claim 67 wherein the at least one state permitting the ~~resource constrained device~~ smart card to transmit messages to the network is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

69. (CURRENTLY AMENDED) The system of Claim 64 of wherein the host computer further comprises logic to operate the host computer according to a

finite state machine having at least one state permitting the ~~resource constrained device~~ smart card to transmit messages to the network wherein the software module is in one of the at least one states permitting the ~~resource constrained device~~ smart card to initiate and send messages.

70. (PREVIOUSLY PRESENTED) The system of Claim 69 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

71. (CURRENTLY AMENDED) The system of Claim 69 wherein the ~~resource constrained device~~ smart card comprises logic to operate the ~~resource constrained device~~ smart card according to a finite state machine having at least one state in which the ~~resource constrained device~~ smart card waits for a message from the host computer indicating that the ~~resource constrained device~~ smart card may transmit a message.

72. (CURRENTLY AMENDED) The system of Claim 64 wherein the ~~resource constrained device~~ smart card further comprises logic to operate the ~~resource constrained device~~ smart card according to a finite state machine whereby ~~the resource constrained device~~ smart card uses the response status at the end of the response to the command sent by the host computer or an intermediate device to indicate that the ~~resource constrained device~~ smart card wants to transmit information to the host computer or to the network.

73. (CURRENTLY AMENDED) The system of Claim 72 wherein the logic to operate the ~~resource constrained device~~ smart card according to a finite state machine further comprises logic to operate the ~~resource constrained device~~ smart card according to a finite state machine having at least one state in which the ~~resource constrained device~~ smart card waits for a message

indicating to the ~~resource constrained device~~ smart card that the ~~resource constrained device~~ smart card may transmit information to the host.

74. (CURRENTLY AMENDED) The system of Claim 73 further the logic to operate the ~~resource constrained device~~ smart card according to a finite state machine further comprises logic to operate the ~~resource constrained device~~ smart card to transition among the states of the finite state machine.

75. (CURRENTLY AMENDED) The system of Claim 72 further comprising:

logic in the host computer or an intermediate device connected between the host computer and the ~~resource constrained device~~ smart card to operate according to a finite state machine to transmit a polling message to the ~~resource constrained device~~ smart card checking if the ~~resource constrained device~~ smart card may want to transmit information to the host computer.

76. (CURRENTLY AMENDED) The system of Claim 75 wherein the host computer or intermediate device includes a Remote Access Server (RAS) and wherein the logic to operate the host computer or intermediate device comprises logic to operate the host computer or intermediate device according to a finite state machine having a Polling state in which the host computer or intermediate device polls the ~~resource limited device~~ smart card, a Get-from-card state in which the host computer or intermediate device obtains packets of data from the ~~resource constrained device~~ smart card, a Putting-to-card state in which the host computer or intermediate device transmits data to the ~~resource constrained device~~ smart card, and a Checking Remote Access Server RAS state in which the host computer or intermediate device checks whether Remote Access Server RAS has any data to transmit to the ~~resource constrained device~~ smart card.

77. (PREVIOUSLY PRESENTED) The system of Claim 76 further comprising logic to operate the host computer or the intermediate device to transition among the states of the finite state machine.

78. (CANCELLED)

79. (CANCELLED)

80. (NEW) A method of secure communication between a MultiMediaCard (MMC) and remote network nodes over a network wherein the MultiMediaCard (MMC) acts as a standalone network node and the remote network nodes communicate with the MultiMediaCard (MMC) using un-modified network clients and servers and wherein the MultiMediaCard (MMC) has a central processing unit, a random access memory, a non-volatile memory, a read-only memory, and an input and output component, comprising:

using a physical link selected from one of several physical link methods;

assigning a unique network address to the MultiMediaCard (MMC) thereby enabling the MultiMediaCard (MMC) to act as a standalone network node;

executing on the MultiMediaCard (MMC) a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with a host computer, operable to communicate with remote network nodes using the networking protocols and operable to implement network security protocols thereby setting a security boundary inside MultiMediaCard (MMC);

implementing an execution model, wherein the communication module is driven by input events and by the applications and wherein the

MultiMediaCard (MMC) optimized memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers;

executing on the host computer one or more communication and networking protocols operable to communicate with the MultiMediaCard (MMC) and operable to communicate with the remote network nodes; and

executing one or more secure network applications on the MultiMediaCard (MMC) wherein the network applications call upon the communication module of the MultiMediaCard (MMC) to communicate with the host computer or the remote network node using the networking protocols and network security protocols and wherein the secure network applications are securely accessible by the remote network nodes using un-modified network clients and servers.

81. (New) A system providing secure communication between a MultiMediaCard (MMC) and remote network nodes over a network wherein the remote network nodes communicate with the MultiMediaCard (MMC) using un-modified network clients and servers and wherein the MultiMediaCard (MMC) has a central processing unit, a random access memory, a non-volatile memory, a read-only memory, and an input and output component, the system comprising:

a physical link connecting the MultiMediaCard (MMC) and a host computer, the physical link selected from one of several physical link methods;

logic to assign a unique network address to the MultiMediaCard (MMC) thereby enabling the MultiMediaCard (MMC) to act as a standalone network node;

the MultiMediaCard (MMC) comprising a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with the host computer, operable to communicate with remote network nodes using the networking protocols and operable to implement network security protocols thereby setting a security boundary inside the MultiMediaCard (MMC), wherein the communication module is driven by input events and by the applications and wherein the MultiMediaCard (MMC) optimizes memory usage by sharing data buffers between one or more communications protocol layers or security protocol layers;

the host computer comprising logic implementing one or more communication networking protocols operable to communicate with the MultiMediaCard (MMC) and operable to communicate with the remote network nodes; and

the MultiMediaCard (MMC) further comprising one or more secure network applications wherein the network applications call upon the communication module of the MultiMediaCard (MMC) to communicate with the host computer or the remote network node using the networking protocols and network security protocols and wherein the secure network applications are securely accessible by the host computer or the remote network nodes using un-modified network clients or servers.

82. (NEW) The method of Claim 80 wherein the physical link is selected from the set including full-duplex serial connection and half-duplex serial connection.

83. (NEW) The method of Claim 82 wherein the physical link is a full-duplex serial connection using the serial peripheral interface protocol.

84. (NEW) The method of claim 80 further comprising connecting an interface device between the smart card and the host computer using a physical link that is a serial connection having half-duplex between the smart card and the interface device and full-duplex between the interface device and the host computer.

85. (NEW) The method of Claim 84 further comprising operating the interface device to perform a bridging function between the half-duplex connection and the full-duplex connection.

86. (NEW) The method of Claim 85 wherein the step of performing a bridging function further comprises providing at least one of function selected from:

enabling a smart card operating in a command/response mode to communicate with network nodes as a peer;

enabling a smart card operating in half-duplex communication mode to handle full-duplex communication traffic;

encapsulating upper layer protocol frames;

enabling transportation of upper layer protocol frames exceeding a frame size limit of the lower link layer; and

supporting multiple logical connections of upper layer protocols.

87. (NEW) The method of Claim 84 of operating a software module on the interface device according to a finite state machine permitting the interface device to forward messages between the smart card and the network wherein the interface device is in one of the at least one states permitting the smart card to initiate and send messages.

88. (NEW) The method of Claim 87 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

89. (NEW) The method of Claim 84 of operating a software module on the host computer according to a finite state machine having at least one state permitting the smart card to transmit messages to the network wherein the software module is in one of the at least one states permitting the smart card to initiate and send messages.

90. (NEW) The method of Claim 89 wherein the at least one state permitting the smart card to transmit messages to the network is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

91. (NEW) The method of Claim 89 comprising the step of operating the smart card according to a finite state machine having at least one state in which the smart card waits for a message from the host computer indicating that the smart card may transmit a message.

92. (NEW) The method of Claim 84 further comprising:

operating the smart card according to a finite state machine whereby the smart card uses the response status at the end of the response to the command sent by the host computer or an intermediate device to indicate that the smart card wants to transmit information to the host computer or to the network.

93. (NEW) The method of Claim 92 wherein the step of operating the smart card comprises operating the smart card according to a finite state machine having at least one state in which the smart card waits for a message

indicating to the smart card that the smart card may transmit information to the host.

94. (NEW) The method of Claim 93 further comprising operating the smart card to transition among the states of the finite state machine.

95. (NEW) The method of Claim 92 further comprising:

operating the host computer or an intermediate device connected between the host computer and the smart card according to a finite state machine to transmit a polling message to the smart card checking if the smart card may want to transmit information to the host computer.

96. (NEW) The method of Claim 95 wherein the host computer or intermediate device includes a Remote Access Server (RAS) and wherein the step of operating the host computer or intermediate device comprises operating the host computer or intermediate device according to a finite state machine having a Polling state in which the host computer or intermediate device polls the smart card, a Get-from-card state in which the host computer or intermediate device obtains packets of data from the smart card, a Putting-to-card state in which the host computer or intermediate device transmits data to the smart card, and a Checking Remote Access Server (RAS) state in which the host computer or intermediate device checks whether Remote Access Server (RAS) has any data to transmit to the smart card.

97. (NEW) The method of Claim 96 further comprising operating the host computer or the intermediate device to transition among the states of the finite state machine.

98. (NEW) The system of Claim 81 wherein the physical link is selected from the set including full-duplex serial connection and half-duplex serial connection.

99. (NEW) The system of Claim 98wherein the physical link is a full-duplex serial connection using the serial peripheral interface protocol.

100. (NEW) The system of Claim 81 further comprising connecting an interface device between the smart card and the host computer using a physical link that is a serial connection having half-duplex between the smart card and the interface device and full-duplex between the interface device and the host computer

101. (NEW) The system of Claim 100 further comprising operating the interface device to perform a bridging function between the half-duplex connection and the full-duplex connection.

102. (NEW) The system of Claim 101 wherein the step of performing a bridging function further comprises providing at least one of function selected from:

enabling a smart card operating in a command/response mode to communicate with network nodes as a peer;

enabling a smart card operating in half-duplex communication mode to handle full-duplex communication traffic;

encapsulating upper layer protocol frames;

enabling transportation of upper layer protocol frames exceeding a frame size limit of the lower link layer; and

supporting multiple logical connections of upper layer protocols.

103. (NEW) The system of Claim 100 of operating a software module on the interface device according to a finite state machine permitting the interface device to forward messages between the smart card and the network wherein the interface device is in one of the at least one states permitting the smart card to initiate and send messages.

104. (NEW) The system of Claim 103 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

105. (NEW) The system of Claim 100 of operating a software module on the host computer according to a finite state machine having at least one state permitting the smart card to transmit messages to the network wherein the software module is in one of the at least one states permitting the smart card to initiate and send messages.

106. (NEW) The system of Claim 105 wherein the at least one state permitting the smart card to transmit messages to the network is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

107. (NEW) The system of Claim 105 comprising the step of operating the smart card according to a finite state machine having at least one state in which the smart card waits for a message from the host computer indicating that the smart card may transmit a message.

108. (NEW) The system of Claim 100 further comprising:

operating the smart card according to a finite state machine whereby the smart card uses the response status at the end of the response to the command sent by the host computer or an intermediate device to indicate that the smart card wants to transmit information to the host computer or to the network.

109. (NEW) The system of Claim 108 wherein the step of operating the smart card comprises operating the smart card according to a finite state machine having at least one state in which the smart card waits for a message indicating to the smart card that the smart card may transmit information to the host.

110. (NEW) The system of Claim 109 further comprising operating the smart card to transition among the states of the finite state machine.

111. (NEW) The system of Claim 108 further comprising:

operating the host computer or an intermediate device connected between the host computer and the smart card according to a finite state machine to transmit a polling message to the smart card checking if the smart card may want to transmit information to the host computer.

112. (NEW) The system of Claim 111 wherein the host computer or intermediate device includes a Remote Access Server (RAS) and wherein the step of operating the host computer or intermediate device comprises operating the host computer or intermediate device according to a finite state machine having a Polling state in which the host computer or intermediate device polls the smart card, a Get-from-card state in which the host computer or intermediate device obtains packets of data from the smart card, a Putting-to-card state in which the host computer or intermediate device transmits data to the smart card, and a Checking Remote Access Server (RAS) state in which the host computer or intermediate device checks whether Remote Access Server (RAS) has any data to transmit to the smart card.

113. (NEW) The method of Claim 112 further comprising operating the host computer or the intermediate device to transition among the states of the finite state machine.

The following is an examiner's statement of reasons for allowance: Applicant has presented very clear and concise statements in the remarks dated September 16, 2008 to distinguish the invention over the prior art, including that the cited art fails to teach or suggest assigning a network address to the smart card thereby enabling it to act as a standalone network node.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432